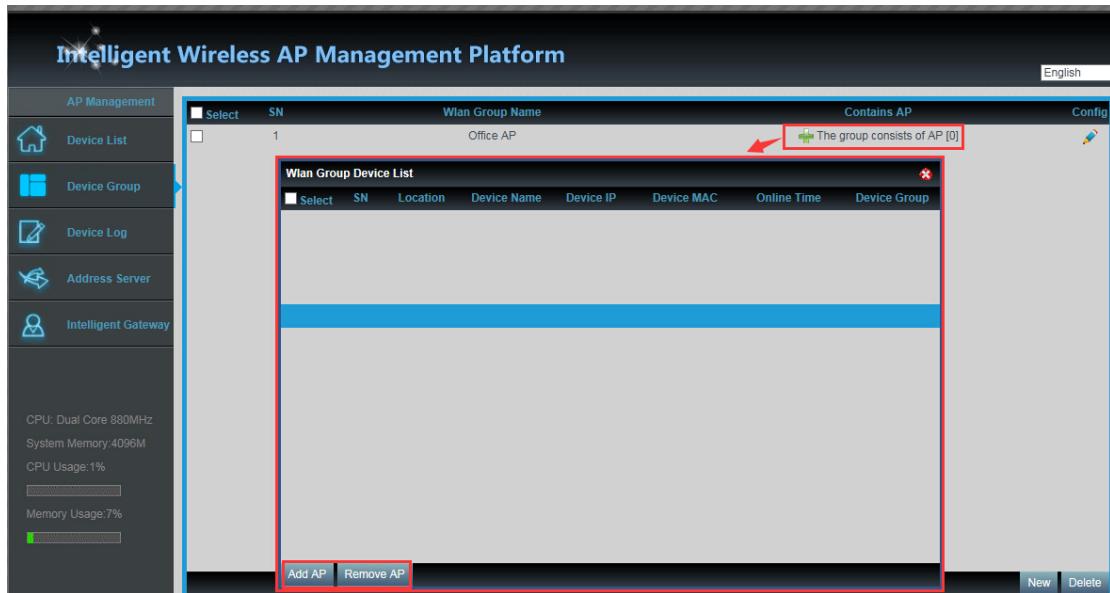


Add /Remove AP into group:

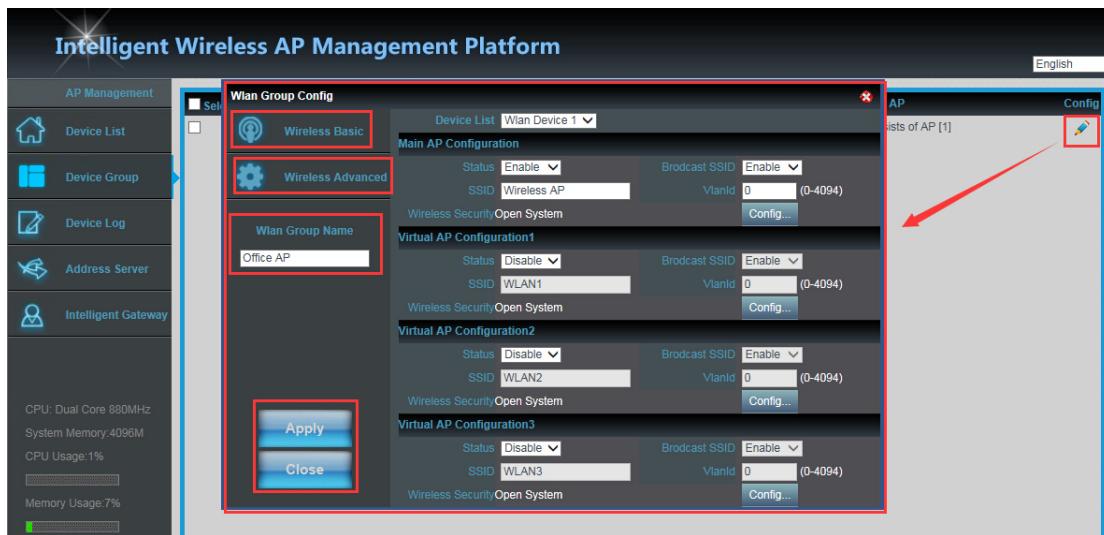
Please follow the steps shown in the following picture:



Configure the AP's data in group:

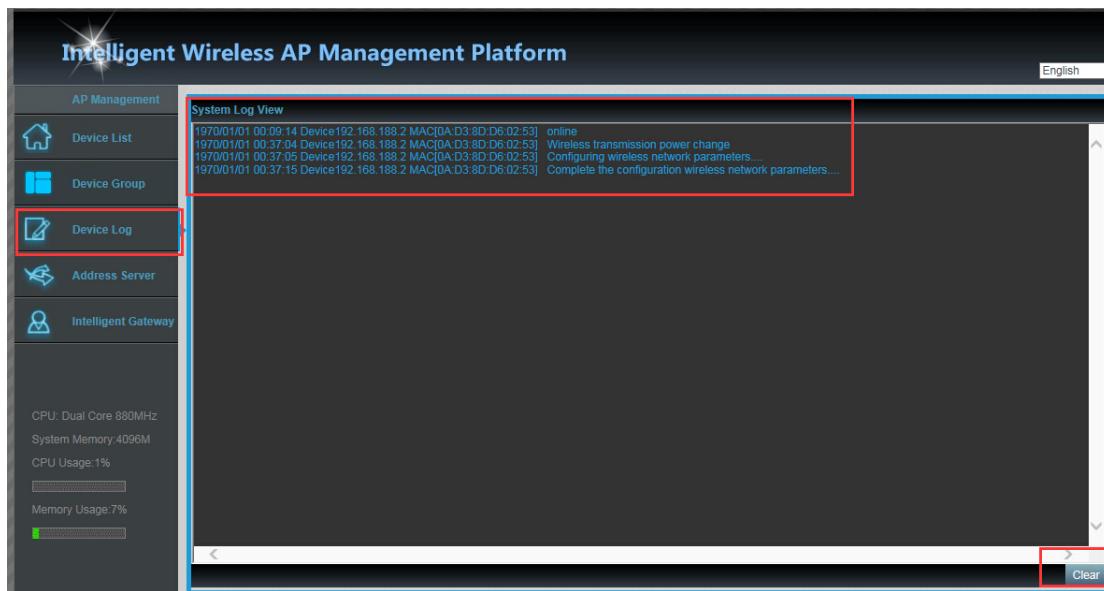
All the data configured here, such as SSID, password, channel... will be applied to all the AP in this group.

Please take the following picture as a reference:



4.3 Device Log

For this log part, record all the AP activities for better technical support.
Can clear it if no need this info.



4.4 Address Server:

Address Server, mean this AC controller can distribute IP address for the Wireless AP connected with this AC controller, to avoid AP's IP address conflict in setup.

Server IP address: mean the server's IP address, if user set is as 192.168.188.1, then AP will get IP address of 192.168.188.X.

Server Address Count: Mean how many AP can connect with this AC controller.

Allocated AP number: Mean QTY of Wireless AP connected into this AC controller.

4.5 Intelligent Gateway

In this part, AC controller work as enterprise router, can access into more than 200 end users.

A. LAN Settings:

Click Intelligent Gateway will automatically jump to the LAN settings

LAN IP Setting:

Set IP address for LAN

Subnet mask

Set Subnet mask for LAN

DHCP Server

DHCP server enable mean it will assign IP address for users.

DHCP Client IP

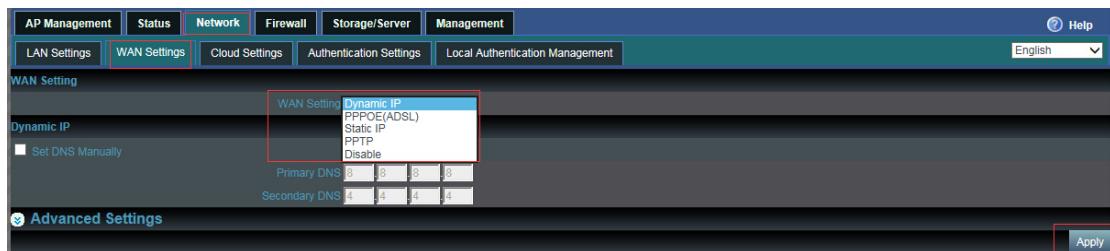
DHCP Client IP mean the IP address range assigned by DHCP Server.

DHCP Lease Time

The networking device get IP lease time from DHCP server.

B. WAN Settings:

In this part, configure the WAN networking mainly.



Dynamic IP:

WAN interface obtains IP and DNS information through DHCP mode.

PPPOE(ADSL):

WAN interface obtains IP and DNS information via PPPOE dial-up mode.

Static IP:

Set IP and DNS information for WAN interface manual

PPTP:

WAN interface obtains IP and DNS information via PPTP mode

MAC Clone:

Specifies the WAN interface MAC, by clicking [Search MAC Address] button, and then will pop up a connected device's MAC, select the MAC desired to clone. You can manually specify the MAC

Enable IGMP Proxy:

Enables IGMP proxy, this feature can be forwarded IGMP data from WAN to the LAN

Enable Ping Address on WAN:

This feature allows outer net to ping WAN

Enable Web Server Address on WAN port

Enable this feature, allows to manage AC3000 from outer net via a specified remote management port

C. Cloud Setting:

Make this AC controller to connect with cloud server for captive portal authentication.

Please note: AC controller can access into cloud server in Gateway operation mode;

Cloud server should support wifidog.

Cloud Server Setting: Enable or Disable.

Cloud Server: Input the cloud server's IP address or domain name.

Login Name: mean the account name in this cloud server.

Contact infomation: pls input if have.

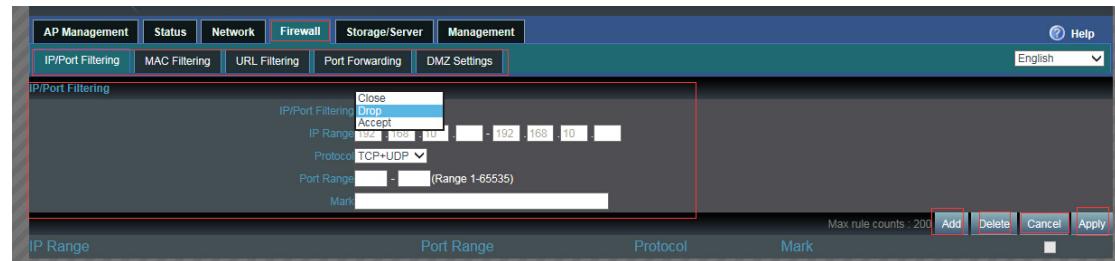
D. Authentication settings and local authentication management.

Make authethnication through the cloud server.

For this part, pls refer to the authentication user manual.

Chapter 5 Firewall

5.1 IP/Port Filtering



IP/Port Filtering

IP/Port forwarding enable, router will limited the data forwarding according to the filtering rule. If the filtering rule is [refuse], then the router will refuse to forward the data in accordance with filtering rule.; If the filtering rule is [allow], the router will forward the data in accordance with filtering rule.

IP Range

Set IP address range

Protocol

Set filtering rule protocol

Port Range

Set filtering port range

Mask

A simple description of the entry rules, for user's easily management;

5.2 MAC Filtering

MAC Filtering

Enabling Mac filtering, router will restrict data forwarding based on the selected filtering rules; When selected Close, router will decline the pointed incoming data; When selected as Open, then router will allow the pointed incoming rules;

Mac address

Set up rules in mac address, users can click Searching Mac Address from the clients in routers, or can set up the mac address manually;

Mask

A simple description of the entry rules, for user's easier management;

5.3 URL Filtering

URL Filtering

Enabling URL filtering, router will restrict access to the pointed URL;

URL address

Set up the declined URL address

5.4 Port Forwarding

Port forwarding

Port forwarding is to forward data from one port to another port, enabling external users have access to an internal private IP in LAN, from an external triggered NAT router ;

Rule Type

Set up rule type, which have specific port number;

Rule name

Port forwarding rule name

LAN IP

IP of the port forwarding

External port

External port number of port forwarding

Internal port

Internal port number of port forwarding

Protocol

Protocol used for port forwarding

5.5 DMZ Settings



DMZ

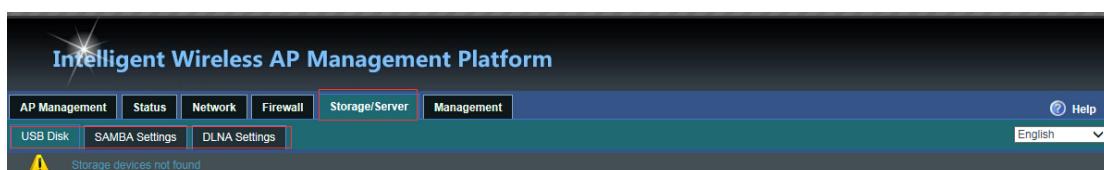
DMZ is short for demilitarized zone; It's a compartment between security zone and non-security zone, in order to solve the problem of external network can not access into internal server after firewall installation; This DMZ zone is a small network zone between external and internal network; While in this small zone, users usually place some open server, like web server, FTP server, or forum; DMZ will protect internal network more efficiently, because this network allocation is another obstacle for hackers, compared to normal firewall

IP LAN IP

IP address of DMZ host

Chapter 6Storage/Server

Before use the storage function, pls make sure insert the USB disk into router, then click Storage, following picture will be showed, there are USB Disk, SAMBA Settings, DLNA settings for choose



A.USB Disk: When insert the USB disk to router's USB port, then will appear following page show the files directory path and partitions name. User can add/delete the files.

B. SAMBA function

We can share the files in USB disk to public users through SAMBA server

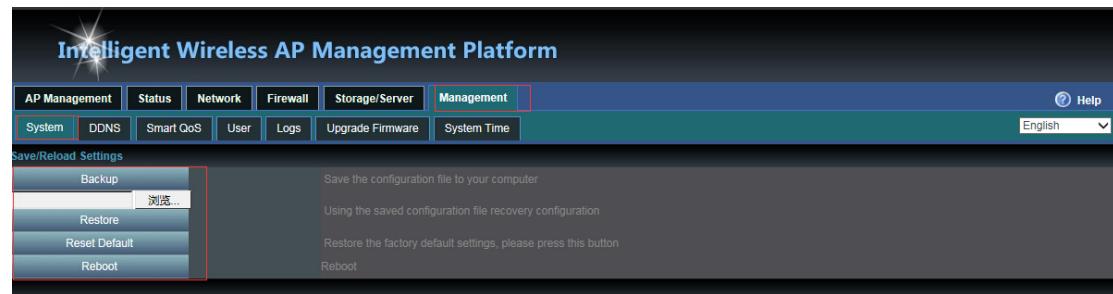
Click SAMBA Settings, then set user name and passwords in wireless router, then apply.

C. DLNA function

User can build a DLNA server through this function. It work with mobile phone or other device support DLNA, then share the files in the local internet.

Chapter 7 Device management

7.1 System management



Backup

Save the configuration files to your computer

Restore

Using the saved configuration file recovery configuration

Reset default

Restore the factory default settings, please press this button

Reboot

Reboot the system

7.2 QoS

The screenshot shows the 'Management' tab selected in the top navigation bar. Under 'Smart QoS', the 'QoS Basic Settings' section is active, featuring a status switch between 'Enable' (selected) and 'Disable'. Below it are input fields for 'Upload' (50000 Kbps) and 'Download' (50000 Kbps). The 'QoS rule setting' section follows, which includes a table for defining bandwidth rules based on IP Address Range or MAC Address. A red box highlights the 'Upload' and 'Download' fields in the 'QoS Basic Settings' section.

Status

Enable or Disable QoS function

Upload

Set up total uploading bandwidth

Download

Set up total downloading bandwidth

IP Address Range

Set up IP range of bandwidth

MAC address

Set up bandwidth control by mac address, user can choose it from Scan MAC, or setup by manual.

Mode

QoS mode settings, shared mode means under the QoS rules, the main PC within all IP range can share the specified bandwidth;

Exclusive mode means single main PC can share the specified bandwidth;

Max bandwidth

Max bandwidth under QoS rules

7.3. DDNS

The screenshot shows the 'Management' tab selected in the top navigation bar. Under 'DDNS', the 'DDNS Settings' section is active, featuring a dropdown menu for 'Dynamic DNS' set to 'Enable'. Below it are input fields for 'User Name' and 'Password/Key'. A red box highlights the 'Dynamic DNS' dropdown and the 'User Name' and 'Password/Key' fields in the 'DDNS Settings' section.

7.4 User management

The screenshot shows the 'User Settings' section of the management interface. The 'User' tab is highlighted. It contains input fields for 'User Name' (admin), 'Password' (*****), and 'Confirm Password'. An 'Apply' button is located at the bottom right.

User Name

Reset new log-in user name

Password

Reset new log-in password

Confirm Password

Comparison to new password, to confirm user input password correctly in two times;

7.5 Device Log

The screenshot shows the 'System Logs' section of the management interface. The 'Logs' tab is highlighted. It includes a 'Status' configuration section with 'Enable' and 'Disable' radio buttons, and a 'Remote Log Service' checkbox. An 'Apply' button is located at the bottom right.

Status

Enable or Disable to show system log

Remote Log Service

To decide whether send System log into some pointed remote server synchronously;

7.6 Upgrade Firmware

This feature allows the device firmware upgrade.

Noted:Upgrading software may cause system outage, In the process of upgrading the firmware, do not power off, otherwise it may damage the AC controller!

The screenshot shows the 'Upgrade Firmware' section of the management interface. The 'Upgrade Firmware' tab is highlighted. It contains a note about software upgrade, a 'Browse...' button for selecting the software file, and a warning note about the upgrade process. An 'Upgrade' button is located at the bottom right.

7.7 System Time

Synchronization with the host

Synchronization time with connected PC and router

Status

Enable or Disable NTP

NTP Server

Select the server time synchronization

Custom NTP Server

Setting user-defined synchronization server IP address

Time Zone

Setting the router's time zone

Please note, System time can work under Gateway operation mode.

And user can set the automatic reboot of this AC controller in system time.

The screenshot shows the 'System Time' configuration page of the management platform. It includes the following settings:

- Status: Enable (radio button selected)
- NTP Server: time.nist.gov
- Custom NTP server: (empty input field)
- Time Zone: (GMT+08:00) Beijing, Chongqing, Guiyang, Urumqi
- When device running at 0:00 Automatic reboot: (checkbox checked)

The 'Apply' button is highlighted with a red box.

Hardware Technical Data

Hardware Data	
Model	AC3000
QTY of manageable AP	Max: 100PCS
CPU	MT7621, 880MHz
FLASH	16M
DDR3	256M
Interface	510/100/1000M Gigabit RJ45 Port 1 Reset Button
Dimension	440mm x200 mm x 45mm
Power	100-240V~ 50/60Hz
power consumption	< 5W
Weight	<2.5KGS
Working Temperature	-20°C ~ 45°C
Working Humidity	10% ~ 90%RH (No condensation)
Storage Temperature	-30°C ~ 70°C
Storage Humanity	5% ~ 90%RH (No condensation)

Note:

This device complies with Part 15 of the FCC Rules.

Operation is subject to the following two conditions:

- (1) this device may not cause harmful interference, and**
- (2) this device must accept any interference received, including interference that may cause undesired operation.**

FCC (additional information)

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.